August 19, 2005

Information Technology Management

Status of Selected DoD Policies on Information Technology Governance
(D-2005-099)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
19 AUG 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology Management: Status of Selected DoD Policies on Information Technology Governance	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **ODIG-AUD (ATTN: AFTS Audit Suggestions),Inspector General of the Department of Defense,400 Army Navy Drive (Room 801),Arlington,VA,22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**35**	

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms

ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
CIO	Chief Information Officer
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
GIG	Global Information Grid
IRM	Information Resource Management
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OMB	Office of Management and Budget

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

August 19, 2005

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/DOD CHIEF INFORMATION OFFICER

SUBJECT: Report on Status of Selected DoD Policies on Information Technology Governance (Report No. D-2005-099)

We are providing this draft report for review and comment. The Under Secretary of Defense for Acquisition, Technology, and Logistics and the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer did not respond to the draft report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. All recommendations remained unresolved. Therefore, we request that the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Assistant Secretary of Defense for Networks and Information Integration Chief Information Officer provide comments on this final report by September 19, 2005.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to AudATM@dodig.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Kathryn Truex at (703) 604-8966 (DSN 664-8966) or Ms. Sarah Davis at (703) 604-9031 (DSN 664-9031). See Appendix F for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Mary L. Ugone
Assistant Inspector General
for Acquisition and Technology Management

Department of Defense Office of Inspector General

Report No. D-2005-099 **August 19, 2005**
(Project No. D2005-D000AL-0100)

Status of Selected DoD Policies on Information Technology Governance

Executive Summary

Who Should Read This Report and Why? The DoD Chief Information Officer, Chief Information Officers of DoD Components, DoD information technology mission area personnel, and other personnel responsible for overseeing DoD information technology requirements should read this report to help the DoD information technology community establish a DoD enterprise-wide information technology governance structure.

Background. Information resource management is the process of managing information resources to accomplish the agency mission. The term encompasses information technology, which is any equipment or interconnected system or subsystem of equipment used in automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this report, we use the terms "information resource management" and "information technology governance" interchangeably.

Congress, through various legislation, requires that information resource management be the primary duty of the DoD Chief Information Officer and that agency heads must delegate specific authorities to the agency Chief Information Officer, including authority to designate a senior agency information security officer. In addition, agencies must use a capital planning and investment control process for selection, management, and evaluation of information technology investments and DoD must establish a specified process to manage its business systems. Office of Management and Budget Circular A-130, "Management of Federal Information Resources," November 28, 2000, requires that agencies use a capital planning and investment control process that links mission needs to information technology and uses portfolios to monitor investments.

Results. DoD is taking steps to enhance its policies for the DoD Chief Information Officer, governance for business systems, information technology portfolio management, and information security, but more work remains to be done. DoD needs to clarify the obligation of DoD Components to implement DoD Chief Information Officer policy, use a standard definition of "system," forward a directive on portfolio management for signature, appoint a permanent employee to the position of senior agency information security officer, and provide oversight of Component compliance with investment review process requirements. See the Finding section of the report for the detailed recommendations.

Management Comments. We provided a draft of this report on July 21, 2005. No management comments were received. Therefore, we request that the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer comment on this final report by September 19, 2005.

Table of Contents

Background

Information Resource Management. Information Resource Management (IRM) is the process of managing information resources to accomplish the agency mission. The term encompasses both the information itself and the related resources such as personnel, equipment, funds, and information technology. Information technology (IT) is defined as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an agency. For purposes of this audit report, we use the terms IRM and IT governance interchangeably. See Appendix C for a synopsis of criteria we used for our audit of selected DoD IT governance policies.

Chief Information Officer. Federal agencies are required to each appoint a Chief Information Officer (CIO). According to Public Law 104-106, "National Defense Authorization Act for Fiscal Year 1996," Division E, Clinger-Cohen Act, section 5125, the primary duty of the CIO of selected agencies, including DoD, is IRM. The CIO must monitor and evaluate agency IT programs and advise the agency head to continue, modify, or terminate the IT programs. In addition, the CIO is to provide advice and assistance to senior management to ensure proper IT acquisition and IRM for the agency.[1] Finally, section 2223, title 10, United States Code (10 U.S.C. 2223), chapter 131, requires the DoD CIO to review and provide recommendations to the Secretary of Defense on DoD budget requests for IT systems and national security systems. See Appendix D for a synopsis of pertinent Federal CIO criteria and see the Finding for pertinent DoD criteria.

Business System Governance. Public Law 108-375, the National Defense Authorization Act for FY 2005, section 332, requires the Secretary of Defense to establish a Defense Business System Management Committee to coordinate DoD business system modernization initiatives and approve certifications for business system modernizations over $1 million. Further, the Secretary of Defense must delegate responsibility and accountability for review, approval, and oversight of planning, design, acquisition, deployment, operation, maintenance, and modernization of DoD business systems to specified approval authorities within DoD. The approval authorities must certify all modernizations over $1 million and must establish an investment review process to review all business systems under their respective purviews.

Portfolio Management. The Clinger-Cohen Act, section 5122, requires agencies to use a capital planning and investment control process to provide for selection, management, and evaluation of IT investments[2]. The Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," November 28, 2000, establishes policy for managing information resources. OMB Circular A-130 requires agencies to manage IT through a capital

[1] These provisions of the Clinger-Cohen Act have been re-codified in title 40 United States Code, subtitle III, section 11315.

[2] These provisions of the Clinger-Cohen Act have been re-codified in title 40 United States Code, subtitle III, section 11312. In addition, section 8401 of Public Law 108-458 amended 40 United States Code, section 11312 to include a requirement for agencies to include information security needs in the agency process for selection of IT investments.

planning and investment control process that links mission needs, information, and IT in an effective and efficient manner and requires the use of portfolios to monitor investments. Finally, the Deputy Secretary of Defense Memorandum "Information Technology Portfolio Management," March 22, 2004, requires that DoD IT investments be managed as portfolios. Portfolio management is defined as management of selected groupings of IT investments using integrated strategic planning, integrated architectures, and performance measures, risk management techniques, transition plans, and portfolio investment strategies.

Information Security. OMB Circular A-130 requires agencies to incorporate security into their information systems. In addition, Public Law 107-347, "E-Government Act of 2002," title III, "Federal Information Security Management Act of 2002," (FISMA) requires Federal agencies to develop, document, and implement an agency-wide information security program and report annually to the Comptroller General and Congress on the adequacy and effectiveness of information security policies, procedures, and practices. The FISMA also requires the heads of Federal agencies to delegate specific authorities to the agency CIO including authority to designate a senior agency information security officer. Finally, Public Law 108-458, "Intelligence Reform and Terrorism Prevention Act of 2004," Section 8401, December 17, 2004, amends the Clinger-Cohen Act to enhance agency planning for information security.

Performance and Accountability Report. The Federal Managers' Financial Integrity Act of 1982 requires Federal agencies to assess the effectiveness of management controls for program, operational, and administrative areas as well as accounting and financial management. OMB Circular A-123, "Management Accountability and Control," June 21, 1995, requires agencies to establish, assess, correct, and report on management controls, and to report annually material weaknesses to the President and Congress. OMB memorandum "FY 2004 Performance and Accountability Reports and Reporting Requirements for the Financial Report of the United States Government," July 22, 2004, provides guidance on preparation and submission of Performance and Accountability Reports which satisfy the requirements of the Federal Managers' Financial Integrity Act of 1982. The 2004 Performance and Accountability Report identified the management of IT and Assurance as an ongoing systemic weakness because DoD information systems are potentially vulnerable to an information warfare attack. In addition, this issue has also been reported as a "significant deficiency" under the reporting requirements of the FISMA.[3]

Objectives

The overall audit objective was to review the DoD governance structure for IT. Specifically, we examined legislative and OMB requirements for IT management, investments, and security; and we determined whether DoD processes were adequate to manage IT. See Appendix A for discussion of scope and methodology. See Appendix B for prior coverage related to these objectives.

[3] A systemic weakness is one that materially affects management controls across organizational and program lines and usually affects multiple DoD components.

Management Control Program Review. DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require each DoD Component to implement a comprehensive system of management controls that provides reasonable assurance that functions are efficiently and effectively carried out as intended and to evaluate the adequacy of the controls. We did not announce the review of the management control program as an audit objective because DoD recognized the management of IT and assurance as an ongoing systemic weakness in the FY 2004 DoD Performance and Accountability report. As indicated in the finding, inadequate DoD policy contributes to the systemic weakness in DoD management of IT as disclosed in the DoD FY 2004 Performance and Accountability Report.

Status of Selected DoD Enterprise-wide Information Technology Governance Policies

Although DoD is making progress, DoD does not have adequate assurance that its information technology is properly managed. This has occurred, in part, because DoD has not fully implemented policies and procedures to establish an effective, enterprise-wide governance structure for managing its information technology. DoD has recently issued policy that partially clarifies the roles pertaining to information technology management; however, until additional policy is issued and existing policy is authoritatively and thoroughly implemented, DoD information technology may not be properly managed to achieve the DoD mission as intended by the Congress and the Office of Management and Budget. Further, inadequate DoD policy contributes to the systemic weakness in DoD management of information technology as disclosed in the DoD FY 2004 Performance and Accountability Report.

DoD CIO Strategic IRM Plan

DoD Strategic IRM Vision. The "DoD CIO Strategic Plan for Information Resources Management (IRM)," June 2004, provides the DoD strategic IRM vision to transition to a global, web-based, or net-centric, environment on a trusted network. The plan seeks to provide a framework for DoD IRM and supporting technologies to achieve the transformation and discusses goals, overarching strategies, principles, and key strategic initiatives. The goals are cascaded down to DoD Components and sub-components that are expected to develop supporting initiatives. DoD has designated the Global Information Grid (GIG) [4] architecture as the organizing construct to achieve net-centric operations and warfare.

Net-Centric Governance. The strategic plan provides a general description of DoD IT governance to achieve net-centricity. Governance is viewed in terms of strategic plans, policies, and forums. Plans provide the vision, goals and objectives; policies provide a means to guide activities; and forums provide oversight, control, and evaluation. In establishing a governance structure for net-centricity, DoD seeks to:

- Emphasize strategic and business planning;
- Leverage existing DoD key decision support systems to the maximum extent possible;

[4] The GIG is the globally interconnected, end–to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG supports all DoD, National Security, and related Intelligence Community missions and functions.

- Use nested and clearly integrated governance processes including integration with key decision support systems;

- Develop new policies and standards as needed based on review of current policies and standards;

- Design net-centric concepts into operations, system, and technical activities, reflect them in architecture, and use the architectures to guide IT investments; and

- Take a portfolio approach to manage and oversee IT investments.

DoD Policy Issues. DoD has outlined a vision to transform to a net-centric information environment and has described a governance structure to achieve the net-centric goal. Policy is an important component of the IT governance structure envisioned by DoD. The following sections discuss some recent developments in selected DoD policy and related guidance pertaining to the DoD CIO, governance for business systems, IT portfolio management, and information security. Also in this report is a synopsis of prior audits covering additional policy concerns that DoD must address before it can establish an effective IRM structure.

DoD CIO

DoD CIO Criteria. Federal criteria regarding the CIO provide that DoD and each Military Department can appoint their own CIO. The DoD CIO must answer to the Secretary of Defense while the Military Department CIOs must answer to the Secretary of their Military Department. However, the criteria do not provide specific explanation of the relationship between the DoD CIO and the Military Department CIOs. DoD criteria provide some insight into the relationship between the DoD CIO and other elements of DoD and the impact on issuance of DoD CIO policy and guidance within DoD.

DoD Directive 8000.1. DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002, establishes policies for DoD IRM, including IT, and requires each DoD Component, including the Military Departments, to have a CIO reporting directly to the Component Head. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, [ASD(C3I)] as the DoD CIO, will serve as the Principal Staff Assistant and issue enterprise-wide policies and procedures on IRM. Component CIOs must advise the DoD CIO and implement DoD CIO policy and guidance.

Deputy Secretary of Defense Memorandum. On May 8, 2003, the Deputy Secretary of Defense issued a memorandum, "Implementation Guidance on Restructuring Defense Intelligence – and Related Matters," that re-designated the position of DoD CIO from ASD(C3I) to the Assistant Secretary of Defense for Networks and Information Integration [ASD(NII)]/DoD CIO answering directly to the Secretary of Defense. The ASD(NII)/DoD CIO was to perform the DoD-wide

CIO duties that were performed by ASD(C3I) as described in DoD Directive 8000.1 and other applicable guidance. The ASD(NII)/DoD CIO has additional responsibility for integrating all information and related activities and services across DoD.

DoD CIO Executive Board. The revised DoD CIO Executive Board (Board) Charter, April 13, 2005, indicates that the Board is the principal DoD forum to advise the DoD CIO on matters pertaining to IT management, the GIG, and the Enterprise Information Environment[5]. The DoD CIO chairs the Board and membership is composed of key representatives from across DoD including the Military Department CIOs. Some key functions of the Board include advising the DoD CIO on information management, IT, and GIG policy; enforcement of a portfolio review process for all IT programs; and alignment of IT portfolios with the GIG. Board members must represent their organization's position with regard to Board issues; convey and support the positions and decisions of the Board to their organizations; and execute actions and tasks as directed by the Chair.

DoD Directive 5144.1. DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005, designates the ASD(NII)/DoD CIO as the Principal Staff Assistant and advisor to the Secretary and Deputy Secretary of Defense for networks, IT, and other designated areas. The DoD CIO is to provide policy, guidance, and oversight for various functional areas under its responsibility and is delegated authority to issue DoD Instructions, publications, and one-time directive-type memoranda to implement policies approved by the Secretary or Deputy Secretary of Defense in areas of assigned responsibility and functions. Instructions to the Military Departments shall be issued through the Secretaries of those departments or their designees. The Secretaries of the Military Departments must ensure that policies and guidance issued by the DoD CIO are implemented in their respective Military Departments. Further, DoD Component Heads must coordinate with the DoD CIO on all matters relating to DoD CIO responsibilities and functions. Finally, the DoD CIO will provide advice to the Office of the Secretary of Defense Principal Staff Assistants on certain DoD-wide issues related to areas under DoD CIO cognizance. See Appendix E for more information on pertinent Principal Staff Assistants.

DoD CIO Policy and Guidance. As previously discussed, policy is an important component of the IT governance structure envisioned by DoD to achieve net-centricity. The DoD CIO is responsible to issue policy on IRM and various functional areas under DoD CIO authority. Military Department CIOs and other Board members have an opportunity to advise the DoD CIO on policy issues through the DoD CIO Executive Board. Recent guidance in DoD Directive 5144.1 requires the Secretaries of the Military Departments to ensure that DoD CIO policy and guidance is implemented in their department and requires Instructions to the Military Department to be issued through the Secretary or their designee. However, the policy does not similarly state that the Principal Staff Assistants and Component Heads must ensure that DoD CIO policy and guidance is implemented. The DoD CIO should ensure that all of its policy and guidance to the Military Departments and other DoD Components is conveyed through the Component Head. In addition, DoD must clarify the obligation of the DoD

[5] The enterprise information environment is the common, integrated computing and communications environment of the GIG and is one of four mission areas in DoD portfolio management.

Principal Staff Assistants and Component Heads to ensure the implementation of DoD CIO policy and guidance. Finally, the DoD CIO must use an effective oversight and enforcement mechanism to ensure that DoD CIO policy and guidance is properly implemented in the Military Departments and across the remainder of DoD to help provide for effective enterprise-wide IRM and achievement of a net-centric information environment.

Governance for Business Systems

National Defense Authorization Act for FY 2005. Public Law 108-375, the National Defense Authorization Act for FY 2005, section 332, requires the Secretary of Defense to establish a Defense Business System Management Committee to coordinate DoD business system modernization initiatives and approve certifications for business system modernizations over $1 million. Further, the Act required the Secretary of Defense to delegate responsibility for review, approval, and oversight of planning, design, acquisition, deployment, operation, maintenance, and modernization of DoD business systems as follows:

- Under Secretary of Defense for Acquisition, Technology, and Logistics shall be responsible and accountable for business systems the primary purpose of which is to support acquisition, logistics, or installations and environment activities of DoD;

- Under Secretary of Defense (Comptroller) shall be responsible and accountable for business systems the primary purpose of which is to support financial management, strategic planning, or budgeting activities of DoD;

- Under Secretary of Defense for Personnel and Readiness shall be responsible and accountable for business systems the primary purpose of which is to support human resource management activities of DoD;

- ASD(NII)/DoD CIO shall be responsible and accountable for business systems the primary purpose of which is to support IT infrastructure or information assurance activities of DoD; and

- Deputy Secretary of Defense or an Under Secretary shall be responsible and accountable for business systems the primary purpose of which is to support DoD activities not covered above.

These approval authorities must certify all modernizations over $1 million for business systems under their respective purviews to the Defense Business System Management Committee. By March 15, 2005, the approval authorities were to establish an investment review process, consistent with section 11312, title 40 U.S.C., to review all business systems under their respective purviews.

Defense Business System Management Committee. On February 7, 2005, the Deputy Secretary of Defense issued a memorandum, "Department of Defense (DoD) Business Transformation," and associated charter, that established the Defense Business System Management Committee to oversee transformation

in the Business Mission Area[6]. The overall goal of the Defense Business System Management Committee is to ensure that the Business Mission Area meets the needs and priorities of the Warfighting Mission Area. In addition, the Defense Business System Management Committee will ensure that business transformation goals are coordinated with DoD strategic planning.

Delegation of Authority. On March 19, 2005, the Deputy Secretary of Defense issued a memorandum, "Delegation of Authority and Direction to Establish an Investment Review Process for Defense Business Systems," that delegated authority for review, approval, and oversight of planning, design, acquisition, deployment, operation, maintenance, and modernization for DoD business systems to the approval authorities described in the National Defense Authorization Act for FY 2005. By March 15, 2005, the approval authorities were to have developed an investment review process that includes review and approval of each DoD business system before obligation of funds on the system.

Investment Review Process. On June 2, 2005, DoD issued the "Investment Review Process Overview and Concept of Operations for Investment Review Boards," to identify processes to establish and operate Investment Review Boards. Each approval authority must charter an Investment Review Board to review business systems supporting activities under its purview. The Investment Review Board reviews the investment and provides a certification recommendation, based on certification criteria, to the cognizant approval authority that then provides certification to the Defense Business System Management Committee. The June 2, 2005 document contains policies to be followed by Office of the Secretary of Defense managed Investment Review Boards. It does not describe Component Investment Review Board processes or business system investment procedures. However, Components are expected to establish their own Investment Review Board processes to manage their business systems transformation activities and ensure National Defense Authorization Act compliance. As DoD implements its investment review process, DoD should ensure that the process provides for review of all business system investments at least annually and DoD should provide oversight of Component compliance with investment review process requirements.

Business Systems Supporting the Infrastructure. The National Defense Authorization Act for FY 2005 identifies business systems supporting the DoD IT and information assurance infrastructure as a subset of business systems and delegates review, approval, and oversight responsibility for them to ASD(NII)/DoD CIO. The ASD(NII)/DoD CIO is required to certify modernizations of these business systems in excess of $1 million to the Defense Business System Management Committee and develop an investment review process. However, in its June 2, 2005, investment review process, DoD states that IT and information assurance infrastructure systems that generally support the DoD Enterprise and all GIG users are not classified as Defense business systems and belong in the Enterprise Information Environment Mission Area. The DoD investment review process does not include business systems supporting the DoD IT infrastructure or information assurance activities.

[6] A Mission Area is a defined area of responsibility whose functions and processes contribute to accomplishment of the mission.

FY 2007 Congressional Reporting. In response to the National Defense Authorization Act for FY 2005, DoD issued its "Status of the Department of Defense's Business Management Modernization Program," March 15, 2005, discussing achievements, plans, commitments, milestones, and performance measures for the DoD Business Management Modernization Program. As one of the program achievements, DoD stated that it had developed a standard definition of a business system to ensure a consistent inventory. However, in the DoD guidance for National Defense Authorization Act Reporting, issued on April 25, 2005, Components were directed to use the Component definition of a system for FY 2007 IT budget purposes resulting in the potential for inconsistent DoD FY 2007 IT budget reporting. On July 18, 2005, the Deputy Assistant Secretary of Defense (Resources) issued a memorandum "OSD Policy for FY07 OMB A-11, Exhibits 53 and 300, and NDAA, Sec 332," which provided Office of the Secretary of Defense policy and guidance for completing the IT budget submissions for FY 2007. The memorandum includes a definition for "defense business system" and includes examples of IT systems that should be included in the definition and examples of IT that should be included as part of another reported system. However, the memorandum applies only to FY 2007 IT budget submissions. DoD must ensure that it uses a standard definition of "system" across the DoD enterprise. In addition, DoD OIG Audit Report No. D-2005-029, "Management of Information Technology Resources Within DoD," January 27, 2005, expressed concerns about the definition of a system within DoD and the DoD ability to develop a system inventory.

IT Portfolio Management

The Clinger-Cohen Act, section 5122, requires agencies to use a capital planning and investment control process to provide for selection, management, and evaluation of agency IT investments.[7] This requirement applies to national security systems to the extent practicable.[8] OMB Circular A-130 requires the use of portfolios as part of the capital planning and investment control process. Finally, the Deputy Secretary of Defense Memorandum "Information Technology Portfolio Management," March 22, 2004, requires that DoD IT investments be managed as portfolios and that guidance in the memorandum be incorporated into the DoD Directive System within 180 days.

Draft DoD Portfolio Management Directive. DoD Draft Directive 8115.aa, "Information Technology Portfolio Management," May 13, 2005, provides policy for managing portfolios of IT investments that focus on improving DoD capabilities and mission outcomes. Portfolios and governance forums must be established at the Enterprise, Mission Area, and Component levels. The ASD(NII)/DoD CIO will establish a governance forum for the Enterprise portfolio, ensure that Mission Area portfolio recommendations are based on architectures that comply with the GIG architecture, and will establish guidance on portfolio management. The draft policy designates leads and portfolio

[7] This provision of the Clinger-Cohen Act has been re-codified in 40 U.S.C., subtitle III, section 11312.

[8] A national security system is any telecommunications or information system operated by the Federal Government the function, operation, or use of which involves intelligence activities, cryptologic activities related to national security, command and control of military forces, equipment that is an integral part of a weapon or weapons system, or is critical to direct fulfillment of military or intelligence missions.

management responsibilities for the Business, Warfighter, Enterprise Information Environment, and DoD portion of the National Intelligence Program Mission Areas and provides portfolio management responsibilities for DoD Components. The portfolio management process for each Mission Area and Component will include monitoring and evaluation of the portfolio in order to recommend continuation, modification, or termination of individual investments. Mission Area recommendations will be provided to and considered within each of the DoD decision support systems. In addition, the Director of Program Analysis and Evaluation will review and issue programming and budgeting guidance that considers Mission Area recommendations to initiate, continue, modify, or terminate funding for IT investments.

Business Mission Area Responsibilities. The Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with ASD(NII)/DoD CIO, Under Secretary of Defense (Comptroller), and the Under Secretary of Defense for Personnel and Readiness, is required to establish a governance forum to oversee portfolio activities in the Business Mission Area in accordance with the National Defense Authorization Act for FY 2005. The Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the other three officials, must also establish a Business Mission Area portfolio, establish guidance for management of the Business portfolio, designate portfolio management responsibilities, and represent Business Mission Area portfolio recommendations within the DoD decision support systems. In addition, three of the business systems approval authorities designated in the National Defense Authorization Act for FY 2005 are to issue portfolio management guidance on the Business Mission Area IT investments supporting activities under their purview and are to conduct portfolio management oversight of their sub-portfolios within the Business Mission Area. The ASD(NII)/DoD CIO, the approval authority for business systems supporting the DoD IT infrastructure and information assurance activities, does not have a sub-portfolio in the Business Mission Area.

Remaining Mission Area Responsibilities. The leads of the three remaining DoD Mission Areas, including ASD(NII)/DoD CIO as the lead for the Enterprise Information Environment Mission Area, will establish the Mission Area portfolio, issue guidance for its management, and establish governance forums to oversee Mission Area portfolio management activities. The Mission Area leads will represent the Mission Area portfolio recommendations within the DoD decision support systems

Component Responsibilities. DoD Component Heads are responsible for establishing Component portfolios aligning to Mission Area portfolio structures and a governance forum to oversee Component portfolio activities. Component Heads must also manage the Component portfolio and ensure that Component IT investments are consistent with Mission Area guidance. Finally, Component CIOs must verify to Mission Area leads and to the ASD(NII)/DoD CIO that Component IT investments are consistent with Mission Area portfolio guidance. Verification includes ensuring that Component resources are applied to Mission Area recommendations that have been approved through the DoD decision support systems.

Implementation of DoD IT Portfolio Management. As DoD implements its portfolio management guidance, it must provide adequate oversight of Component IT investments to validate that Components are following portfolio

management guidance and recommendations of the Mission Area. Requiring the DoD Component Heads to ensure that Component IT investments are consistent with Mission Area guidance and having Component CIOs verify this to the Mission Areas and ASD(NII)/DoD CIO are positive steps. However, the draft portfolio management guidance does not indicate what specific proactive steps the Mission Areas will take to gain sufficient visibility into Component IT investments to validate that Component investments are consistent with Mission Area guidance and recommendations. Such steps could include Mission Area lead review and comment on DoD IT budget requests for investments within their Mission Area portfolio. These budget reviews by the Mission Areas could assist the DoD CIO in fulfilling its responsibility under chapter 131, 10 U.S.C. 2223 to review and provide recommendations to the Secretary of Defense on DoD budget requests for IT systems and national security systems.

Information Security

The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, availability, and authentication.

Federal Information Security Management Act. Public Law 107-347, the E-Government Act of 2002, Title III, FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. It requires Federal agencies to develop, document, and implement an agency-wide information security program and report annually to the Comptroller General and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

Authority of DoD Chief Information Officer. FISMA requires the head of each Federal agency to delegate authority to the agency CIO to ensure compliance with the requirements of the Act. These requirements specifically include:

- designating a senior agency information security officer,
- developing and maintaining an agency-wide information security program,
- developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, and
- assisting senior agency officials concerning their responsibilities.

The position of DoD CIO was established in response to the requirements issued under the National Defense Authorization Act for FY 1996. FISMA was enacted in December 2002 and set forth specific instruction for the head of each agency to delegate authority to the CIO to ensure compliance with the requirements imposed on the agency. Therefore, FISMA instructs the Secretary of Defense to delegate to the CIO the authority to ensure compliance with subchapter III of 44 U.S.C chapter 35. DoD Directive 5144.1, "Assistant Secretary of Defense for

Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005, charters the ASD(NII)/DoD CIO responsibilities and functions. The DoD OIG commented on the draft of this directive on November 2, 2004, and based on that coordination, DoD Directive 5144.1 delegates to the DoD CIO the responsibility to fulfill the requirements in 44 U.S.C. 3544. The DoD CIO must use an effective oversight and enforcement mechanism to ensure that the directive is properly implemented across the DoD enterprise.

Senior Agency Information Security Officer. FISMA requires the DoD CIO to designate a senior agency information security officer who shall:

- carry out the CIO responsibilities included in FISMA,
- possess professional qualifications, including training and experience, required to administer the functions described in FISMA,
- have information security duties as that official's primary duty, and
- head an office with the mission and resources to assist in ensuring agency compliance with FISMA.

On April 19, 2005, the Acting DoD CIO signed a memorandum designating the Director, Information Assurance, Office of the Deputy Chief Information Officer, as the senior agency information security officer. DoD filled the FISMA-required position of a senior agency information security officer with a temporary employee for a one year tour length with a one year optional extension. As of August 2005, DoD has not provided a final delegation of authorities as they relate to the required position.

Section 3544(a)(5) of title 44, United States Code requires the CIO report annually on the effectiveness of the agency information security program and on the progress of remedial actions. Since one goal of designating a senior agency information security officer is to assist the CIO in carrying out his or her FISMA responsibilities, the continued appointment of the senior agency information security officer on a temporary basis would lack the continuity of oversight that FISMA intends.

Additional DoD Policy Concerns

The previous sections discussed recent DoD policy developments and concerns in the areas of the DoD CIO, governance for business systems, IT portfolio management, and information security. Recent audits have identified additional policy concerns that DoD must address as it continues to build and define its IRM process.

GIG Implementation. The GIG is the DoD organizing construct to achieve net-centric operations and warfare; however, in Government Accountability Office (GAO) Report No. GAO-04-858, "Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation," July 28, 2004, GAO expressed uncertainty on how DoD will execute its plans and make

the GIG a reality. The GAO concerns included the key areas of enforcing GIG decisions across the military services and evaluating the progress of the GIG. The report contained no recommendations but indicated that GAO would perform future audits of the subject.

System Interoperability and GIG Inventory. Policy is an important component of the governance structure envisioned by DoD to achieve net-centricity, and interoperability and information assurance are important elements in achieving the DoD strategic goal of net-centricity. DoD OIG Report No. D-2005-033, "Implementation of Interoperability and Information Assurance Policies for Acquisition of Navy Systems," February 2, 2005[9], indicated that the Navy had not fully implemented DoD interoperability policy. This audit demonstrates the challenges of implementation and enforcement of DoD policy at the Component level. Further, the audit found that DoD had not issued clear guidance on populating and maintaining the asset inventory for the GIG resulting in the lack of a complete GIG inventory at the Component level and inability of DoD to obtain adequate information superiority.

IT Investment Reporting. Submitting IT investment reports (Exhibit 300 Reports) to OMB is required by OMB Circular A-11 for budget requests. Congress has challenged, in Committee report language, the quality of DoD IT management because IT documents and associated budget data provided by DoD were inaccurate, misleading, or incomplete. Based on the results in DoD OIG Report No. D-2004-081, "Reporting of DoD Capital Investments for Information Technology," May 7, 2004; D-2005-02, "Reporting of DoD Capital Investments for Technology in Support of FY 2005 Budget Submission," October 12, 2004; and DoD OIG Report No. D-2005-083, "Reporting of DoD Capital Investments for Information Technology in Support of the FY 2006 Budget Submission," June 10, 2005. DoD Components did not adequately report IT investments in the budget requests for FY 2004 through FY 2006. This occurred because the Component CIOs and Chief Financial Officers did not include all of the required information in the submission reports. A particularly glaring omission was information pertaining to security and privacy.

DoD Systems Inventory. DoD needs a complete inventory of information systems to prepare accurate systems status responses to OMB and congressional inquiry. Based on results in DoD OIG Report No. D-2005-029, "Management of Information Technology Resources Within DoD," January 27, 2005, DoD has not established a complete inventory of its information systems or consistently defined an information system. Without a complete inventory of information systems, DoD can not efficiently plan for future enhancements or replacements of systems, report accurately on DoD expenditure for IT, or report accurately on system security status.

Current DoD Accreditation Process. 44 U.S.C. section 3543 delegates DoD the responsibility to ensure that its Components comply with the National

[9] This audit report was one of a series of audits on implementation of interoperability and information assurance policies for acquisition of DoD systems. For additional details, see DoD OIG Report No. D-2003-011, "Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems," October 17, 2002, DoD OIG Report No. D-2004-008, "Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems," October 15, 2003, and DoD OIG Report No. D-2005-034, "Interoperability and Information Assurance Policies for Acquisition of Air Force Systems," February 2, 2005.

Institute of Standards and Technology (NIST) standards; however, DoD OIG Report No. D-2005-054, "DoD Information Technology Security Certification and Accreditation process," April 28, 2005, found that OASD(NII)/CIO officials did not agree with this interpretation and therefore did not update DoD policy and processes to include guidance established by NIST. Continued failure to do so will result in potential information assurance incompatibilities between DoD and other executive agencies.

Proposed DoD Accreditation Process. To achieve adequate security commensurate with the level of risk, OMB Circular A-130 states that agencies must comply with OMB policy and NIST guidance, even if an agency implements its own security standards. Also, the FISMA, December 17, 2002, requires an annual report to the Comptroller General and Congress on the agency's development, documentation, and implementation of its agency-wide information security program. DoD OIG Report No. D-2005-094, "Proposed DoD Information Assurance Certification and Accreditation Process," July 21, 2005, concluded that draft DoD Instruction 8510.bb, "DoD Information Assurance Certification and Accreditation Process (DITSCAP)," does not implement the reaccredidation, security weakness, system user, and control objective requirements established by FISMA and OMB.

Plans of Action and Milestones. The OMB FISMA guidance requires agencies to prepare a Plan of Action and Milestones for all program and system security weaknesses. The DoD OIG Report No. D-2005-023, "Assessment of DoD Plan of Action and Milestones Process," December 13, 2004, concluded that DoD did not develop, implement, manage and report Plans of Action and Milestones for all IT security weaknesses. After mediation between DoD OIG and DoD Management, it was agreed, in June 2005, that the ASD(NII)/DoD CIO will issue a DoD policy memorandum that will establish a comprehensive Plan of Action and Milestones process to develop, implement, manage, and close identified security performance weaknesses. The guidance in the memorandum will subsequently be incorporated into a change to DoD Instruction 8500.2, "Information Assurance (IA) Implementation".

IT Security Training and Awareness. The FY 2004 FISMA reporting process included questions on specialized training for employees with significant IT security responsibilities and security awareness training for agency employees. According to DoD OIG Report No. D-2005-025, "DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness," December 17, 2004, the DoD CIO did not ensure the accuracy and supportability of the training information reported by DOD Components in response to FISMA. In particular, the DoD CIO did not ensure that DoD Components defined and identified employees with significant IT security responsibilities, developed training requirements for those professionals, and established processes to track and monitor either security awareness training or specialized security training.

Since recommendations were made in the above reports, we did not make additional recommendations in this report.

Conclusion

DoD has outlined a vision to transform to a net-centric information environment. As DoD notes in its strategic IRM plan, achievement of the net-centric vision will take years to complete and involve periodic restructuring and redirection. An effective IRM process is critical to accomplishment of net-centricity for DoD; however, establishment of an effective enterprise-wide IRM process for DoD is a monumental challenge that requires a concerted effort throughout the Department. Policy is an important component of the governance structure envisioned by DoD to achieve net-centricity. DoD is taking steps to enhance policies concerning the DoD CIO, governance for business systems, IT portfolio management, and information security, but more work remains to be done. For example, DoD has recently updated policy on the DoD CIO; however, DoD needs to further clarify requirements for DoD Components to follow DoD CIO policy and guidance and must use management oversight and enforcement mechanisms to verify that DoD CIO policy and guidance are properly implemented across the DoD enterprise. Use of such a function is inherently a management responsibility. In addition, DoD has also begun to implement National Defense Authorization Act for FY 2005 requirements for governance of DoD business systems; however, DoD needs to provide oversight of Component compliance with investment review process requirements. Further, DoD must issue final policy on IT portfolio management and provide sufficient oversight to validate that DoD Component actions are consistent with Mission Area portfolio guidance and recommendations. Finally, DoD has delegated responsibility to the DoD CIO based on FISMA; however, DoD must appoint a permanent employee to the position of senior agency information security officer. Improvements in and proper implementation of the above DoD policies will help DoD to establish an IT governance structure, including associated management controls, that is more consistent with the requirements of the Clinger-Cohen Act, National Defense Authorization Act for FY 2005, and FISMA, than is present practice.

Recommendations

1. We recommend that the Assistant Secretary of Defense for Networks and Information Integration/DoD CIO:

a. Prepare a memorandum for signature by the Deputy Secretary of Defense clarifying the obligation of DoD Principal Staff Assistants and Component Heads, similar to the obligation imposed upon Secretaries of the Military Departments by DoD Directive 5144.1, to implement DoD Chief Information Officer policy and guidance.

b. Ensure that the clarification accomplished by Recommendation 1.a. is included in the next change request for DoD Directive 5144.1.

c. Ensure that DoD Chief Information Officer policy and guidance is directed to Secretaries of the Military Departments and DoD Component Heads, to include the Chairman of the Joint Chiefs of Staff and the Combatant Commands, to ensure accountability and compliance.

d. Use effective management oversight and enforcement mechanisms to verify that its policies and guidance are properly implemented by the Military Departments and the remainder of the DoD enterprise.

e. Subject to accomplishment of Recommendation 1.a., require DoD Components to use a standard definition of "system" across the DoD enterprise for FY 2007 and subsequent year information technology budget reporting and other purposes.

f. Provide specific steps that Mission Areas must take to gain visibility into Component information technology investments to validate that Component investments are consistent with Mission Area guidance and recommendations.

g. Complete the staffing process and forward a portfolio management directive to the Deputy Secretary of Defense for signature in order to assist in the establishment of a consistent governance structure across the DoD enterprise.

h. Appoint a permanent Office of the Assistant Secretary of Defense for Networks and Information Integration employee to the position of senior agency information security officer as required by the Federal Information Security Management Act.

2. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics specify the processes that will be followed to provide oversight to ensure that Components establish Investment Review Boards and manage their business system transformation activities in accordance with the National Defense Authorization Act and other criteria as required by the June 2, 2005 "Investment Review Process Overview and Concept of Operations for Investment Review Boards."

Management Comments Required

The Under Secretary of Defense for Acquisition, Technology, and Logistics and the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer did not comment on the draft of this report. We request that the Under Secretary and Assistant Secretary provide comments on the final report.

Appendix A. Scope and Methodology

We reviewed recent developments in DoD policy and related guidance pertaining to elements of IT governance within DoD. Specifically, we reviewed the DoD CIO IRM strategic plan to identify the DoD strategic vision. We also reviewed the Paperwork Reduction Act, Clinger-Cohen Act, Executive Order 13011, OMB Circular A-130, DoD Directive 8000.1, and DoD Directive 5144.1 to clarify the role and authority of the DoD CIO. In addition, we reviewed the National Defense Authorization Act for FY 2005 and overall DoD implementation of key requirements for governance of DoD business systems. Further, we reviewed OMB Circular A-130 discussion on portfolios and draft DoD policy to implement IT portfolio management. Finally, we reviewed the FISMA, DoD Directive 5144.1, and related DoD efforts to implement key information security requirements. We reviewed documentation dated from October 1994 through July 2005.

We visited or contacted officials from the Office of the ASD(NII)/DoD CIO and the CIOs of the Army, Navy, and Air Force.

We performed this audit from December 2004 through July 2005 in accordance with generally accepted government auditing standards.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Use of Legal Assistance. We performed this audit with advice from the Office of Legal Counsel for the DoD Inspector General on matters pertaining to compliance with Public Law and U.S.C.

GAO High-Risk Area. The GAO had identified several high-risk areas throughout the Federal Government. This report provides coverage of the high-risk areas related to Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures. In addition, GAO identified several high-risk areas within DoD. This report provides coverage of the area related to the DoD Approach to Business Transformation.

Appendix B. Prior Coverage

During the last 5 years, the GAO and the DoD OIG have issued 23 reports on pertinent IT management issues. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD OIG reports can be accessed at http://www.dodig.osd.mil/audit/reports.

GAO

GAO Report No. GAO-05-381, "DoD Business Systems Modernization: Billions Being Invested without Adequate Oversight," April 29, 2005

GAO Report No. GAO-04-858, "Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation," July 28, 2004

GAO Report No. GAO-04-376, "Information Security: Agencies Need to Implement Consistent Processes In Authorizing Systems for Operation," July 28, 2004

GAO Report No. GAO-04-823, "Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure and Challenges," July 21, 2004

GAO Report No. GAO-04-907T, "Department of Defense: Long-standing Problems Continue to Impede Financial and Business Management Transformation," July 7, 2004

GAO Report No. GAO-04-615, "DoD Business Systems Modernization: Billions Continue to Be Invested with Inadequate Management Oversight and Accountability," May 27, 2004

GAO Report No. GAO-04-731R, "DoD Business System Modernization: Limited Progress in Development of Business Enterprise Architecture and Oversight of Information Technology Investments," May 17, 2004

GAO Report No. GAO-04-551T, "Department of Defense: Further Actions Needed to Establish and Implement a Framework for Successful Financial and Business Management Transformation," March 23, 2004

GAO Report No. GAO-04-115, "Information Technology: Improvements Needed in the Reliability of Defense Budget Submissions," December 19, 2003

DoD IG

DoD IG Report No. D-2005-094, "Proposed DoD Information Assurance Certification and Accreditation Process," July 21, 2005

DoD IG Report No. D-2005-083, "Reporting of DoD Capital Investments for Information Technology in Support of the FY 2006 Budget Submission," June 10, 2005

DoD IG Report No. D-2005-054, "DoD Information Technology Security Certification and Accreditation Process," April 28, 2005

DoD IG Report No. D-2005-033, "Implementation of Interoperability and Information Assurance Policies for Acquisition of Navy Systems," February 2, 2005

DoD IG Report No. D-2005-034, "Implementation of Interoperability and Information Assurance Policies for Acquisition of Air Force Systems," February 2, 2005

DoD IG Report No. D-2005-029, "Management of Information Technology Resources Within DoD," January 27, 2005

DoD IG Report No. D-2005-025, "DoD FY 2004 Implementation of the Federal Information Security Management Act for Information Technology Training and Awareness," December 17, 2004

DoD IG Report No. D-2005-023, "Assessment of DoD Plan of Action and Milestones Process," December 13, 2004

DoD IG Report No. D-2005-002, "Reporting of DoD Capital Investments for Technology in Support of FY 2005 Budget Submission," October 12, 2004

DoD IG Report No. D-2004-081, "Reporting of DoD Capital Investments for Information Technology," May 7, 2004

DoD IG Report No. D-2004-008, "Implementation of Interoperability and Information Assurance Policies for Acquisition of Army Systems," October 15, 2003

DoD IG Report No. D-2003-117, "Systems Inventory to Support the Business Enterprise Architecture," July 10, 2003

DoD IG Report No. D-2003-022, "FY 2002 Independent Assessment of the DoD Subset of Information Technology Systems for Government Information Security Reform Reported for FY 2001," November 14, 2002

DoD IG Report No. D-2003-011, "Implementation of Interoperability and Information Assurance Policies for Acquisition of DoD Weapon Systems," October 17, 2002

Appendix C. Information Technology Governance Criteria

We reviewed a variety of criteria pertaining to elements of IT governance. Specifically, we reviewed criteria on the CIO, DoD business system governance, IT portfolio management, and information security. See Appendix D for additional details on criteria for the CIO. The following discussion synopsizes criteria we reviewed from the U.S.C., Public Law, President, OMB, and DoD.

United States Code

Title 40, United States Code. Chapter 113, Responsibility for Acquisitions of Information Technology, subtitle III, Title 40 U.S.C. covers responsibilities for executive agencies' capital planning and investment control in Section 11312, and the Agency CIO in Section 11315.

Section 11312. Section 11312 of title 40, United States Code states that in fulfilling the responsibilities assigned under 44 U.S.C. 3506, section (h) , the head of each executive agency shall design and implement in the executive agency a process for maximizing the value, and assessing and managing the risks, of the IT acquisitions of the executive agency.

Section 11315. Section 11315 of title 40, United States Code establishes the authority and responsibility of Executive Agency CIOs, such as, providing advice or other assistance to head or senior personnel of each executive agency, developing, maintaining, and facilitating the implementation of a sound IT architecture, and promoting the effective and efficient design and operation of all major IRM processes for the executive agency. The CIO's primary duty is IRM, through monitoring, and evaluating IT programs, and advising the agency head to continue, modify, or terminate those IT programs.

Title 44, United States Code. Chapter 35, Coordination of Federal Information, of title 44, United States Code covers Federal Information Policy in subchapter I Section 3506 and Information Security in subchapter III Sections 3543 and 3544.

Section 3506. Section 3506 of title 44, United States Code states that the agency CIO shall report directly to the agency head and carry out the responsibilities listed under subchapter I of 44 U.S.C. 3506. Also, the Secretary of Defense and the Secretaries of each Military Department may each designate CIOs who shall report directly to such Secretary and carry out the responsibilities of the Department listed under Subchapter I of 44 U.S.C. 3506. Finally, if more than one CIO is designated, the respective duties shall be clearly delineated.

Section 3543. Section 3543 of title 44, United States Code designates that the Director of OMB is responsible for developing and overseeing the implementation of policies, principles, standards, and guidelines including through ensuring timely agency adoption of and compliance with the standards issued under 40 U.S.C. 11331. Also, the Director of OMB shall require agencies to identify and provide information security protections commensurate with the

risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected by an agency or information systems used by an agency, contractor of an agency, or other organization on behalf of the agency.

Section 3544. Section 3544 of title 44, United States Code states that the Head of each agency is responsible for providing information security protection commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected by an agency or information systems used by an agency, contractor of an agency, or other organization on behalf of the agency. Also, the Head of each agency shall comply with all the requirements in subchapter III of title 44, United States Code and section 11331 of title 40, United States Code.

Public Law

Paperwork Reduction Act of 1995. Public Law 104-13, the Paperwork Reduction Act of 1995 assigns Federal agencies IRM responsibilities to increase agency productivity, efficiency, and effectiveness. The agency will also establish a senior official to carry out these responsibilities. The Secretary of Defense and the Secretaries of each Military Department may designate a senior official to carry out the IRM responsibilities.

Clinger-Cohen Act. Public Law 104-106, the National Defense Authorization Act for FY 1996, Division E, the Clinger-Cohen Act, provides duties for the agency CIO. The CIO of selected agencies, including DoD, will have IRM as their primary duty. Additional duties include evaluating IT investments and advising the agency head on management for these IT investments.

National Defense Authorization Act for FY 1999. Public Law 105-261, the National Defense Authorization Act for FY 1999, Subtitle D amends chapter 131 of title 10, United States Code by adding a new section 2223 "Information technology: additional responsibilities of Chief Information Officers." Section 2223 provides DoD CIO responsibilities in addition to those in the Clinger-Cohen Act, including review of IT budget requests and ensuring interoperability.

Federal Information Security Management Act. Public Law 107-347, the E-Government Act of 2002, Title III, FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.

National Defense Authorization Act for FY 2005. Public Law 108-375, the National Defense Authorization Act for FY 2005, section 332 requires the Secretary of Defense to establish a Defense Business System Management Committee to coordinate DoD business systems modernization initiatives, and certify and approve investments in excess of $1M. This Act requires the Secretary of Defense to assign certain responsibilities to specific Under Secretaries of Defense. In addition, the ASD(NII/CIO) is specifically made responsible for business systems that support the DoD IT infrastructure or information assurance activities.

The President

Executive Order 13011. Executive Order 13011, "Federal Information Technology," July 16, 1996 establishes that agency CIOs have the visibility and responsibility to advise agency heads on design, development, and implementation of information systems. Furthermore, the agency CIO must review, monitor, and evaluate information systems and advise the agency head whether to modify or terminate those systems. These requirements must remain consistent with the applicability of the Information Technology Act.

Office of Management and Budget

OMB Circular A-130. OMB Circular A-130, Management of Federal Information Resources," November 28, 2000**,** was issued in accordance with the Paperwork Reduction Act, Clinger-Cohen Act, and Executive Order 13011. The OMB Circular A-130 establishes policy for management of federal information resources. The circular requires agencies to manage IT using a capital planning and investment control process that includes use of portfolios. The circular also requires agencies to appoint a CIO.

Department of Defense

DoD Directive 8000.1. DoD Directive 8000.1, "Management of DoD Information Resources and Information Technology," February 27, 2002, establishes policy for DoD IRM, and requires each DoD Component, including Military Departments, to have a CIO reporting directly to the Component Head. Deputy Secretary of Defense Memorandum dated May 8, 2003, states that the position of C3I/DoD CIO has been changed to ASD(NII)/DoD CIO. This memorandum also delegates additional responsibilities to the CIO for integrating IT activities across the Department and adhering to the instruction provided in DoD Directive 8000.1.

DoD Instruction 8500.2. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003 implements policy and prescribes procedures under DoD Directive 8500.1. New Plan of Action and Milestones guidance will be incorporated into this Instruction.

Memorandum on Restructuring Defense Intelligence. Deputy Secretary of Defense Memorandum, "Implementation Guidance on Restructuring Defense Intelligence – and Related Matters," May 8, 2003, redesignated the position of DoD CIO from ASD(C3I) to the (ASD(NII))/DoD CIO. This memorandum also states that the position of ASD(NII)/DoD CIO has the same responsibilities as the ASD(C3I)/DoD CIO and increased responsibilities for integrating all information and related activities across the Department. Also, this memorandum states that the ASD(NII)/DoD CIO must perform the DoD-wide duties described in DoD Directive 8000.1, and if necessary, update any existing DoD Directives or Instructions in order to implement this Memorandum.

Memorandum on IT Portfolio Management. Deputy Secretary of Defense Memorandum "Information Technology Portfolio Management," March 22, 2004, states that IT investments be managed as portfolios and guidance has to be incorporated into the DoD Directive System within 180 days.

DoD Business Transformation. Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Business Transformation**,"** February 7, 2005, established the Defense Business Systems Management Committee to oversee the transformation in Business Mission Area, including its priorities, goals, and responsibilities.

Delegation of Authority for Defense Business Systems. Deputy Secretary of Defense Memorandum, "Delegation of Authority and Direction to Establish an Investment Review Process for Defense Business Systems," March 19, 2005, delegates authority for review, approval, and oversight of planning, design, acquisition, deployment, operations, maintenance, and modernization of DoD business systems to the approval authorities listed in National Defense Authorization Act for FY 2005.

DoD CIO Executive Board Charter. The revised DoD CIO Executive Board Charter, April 13, 2005, states that the DoD CIO Executive Board is the principal forum to advise the DoD CIO on matters pertaining to IT management, GIG policy, alignment of IT portfolios with the GIG, and the Enterprise Information Environment. This Board is chaired by the DoD CIO, and membership is composed of representatives from DoD Components, including the Military Department CIOs.

DoD Directive 5144.1. DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)," May 2, 2005, provides responsibilities for the DoD CIO. The DoD CIO must provide policy, guidance, and oversight for various functional areas under its responsibility. The Secretaries of the Military Departments must ensure that DoD CIO policy and guidance is implemented in their respective Military Department.

DoD Draft Directive 8115.aa. DoD Draft Directive 8115.aa, "Information Technology Portfolio Management," May 13, 2005 provides policy for management of DoD IT investments as portfolios and requires all four DoD Mission Areas to develop and manage portfolios and establish governance forums to oversee their portfolio activities. Further, DoD Components are to develop portfolios aligned with Mission Area portfolio structures and ensure Component IT investments are consistent with Mission Area portfolio guidance.

Appendix D. Federal Criteria on Chief Information Officer

Since at least 1995, the President, Congress, and OMB have issued requirements for Federal agencies to perform IRM activities. The following criteria, in chronological order, emphasize the key role of the agency CIO in implementing agency IRM.

Paperwork Reduction Act of 1995. Public Law 104-13, the Paperwork Reduction Act of 1995, May 22, 1995, assigns Federal agencies IRM responsibilities to improve agency productivity, efficiency, and effectiveness. Each agency must designate a senior official reporting directly to the agency head to carry out agency IRM responsibilities. The Secretary of Defense and the Secretary of each Military Department may each designate senior officials who report directly to such Secretary to carry out the IRM responsibilities for DoD. If more than one official is designated, the respective duties of the officials shall be clearly delineated.

Clinger-Cohen Act. Public Law 104-106, the National Defense Authorization Act for FY 1996, Division E, the Clinger-Cohen Act, February 10, 1996, section 5125 (a) indicates that the agency senior officials referred to in the Paperwork Reduction Act of 1995 will be called CIOs. Section 5125 (b) provides that each agency CIO will provide advice and assistance to the agency head and other senior management on IT acquisition and IRM. The CIO should also develop, maintain, and facilitate implementation of a sound and integrated IT architecture to help achieve agency IRM goals and strategic goals. In addition, Section 5125 (c) provides that CIOs of selected agencies, including DoD, will have IRM as their primary duty, monitor and evaluate performance of agency IT programs, and advise the agency head on whether to continue, modify, or terminate a program or project.[10] These requirements also apply to national security systems.

Executive Order 13011. Executive Order 13011, "Federal Information Technology," July 16, 1996, required Federal agencies to establish clear accountability for IRM activities by creating CIOs with the visibility and management responsibilities to advise the agency head on design, development, and implementation of information systems. The CIO must monitor and evaluate performance of information systems and, as necessary, advise the agency head to modify or terminate those systems. These requirements apply to national security systems in a manner consistent with applicability in the Clinger-Cohen Act.

Section 2223, title 10, United States Code. Public Law 105-261, the National Defense Authorization Act for FY 1999, October 17, 1998 added section 2223, "Information technology: additional responsibilities of the Chief Information Officers," to chapter 131, title 10, United States Code. Section 2223 required the DoD CIO to review and provide recommendations to the Secretary of Defense on DoD budget requests for IT and national security systems and ensure interoperability of IT and national security systems throughout DoD. In addition,

[10] Provisions of section 5125 (b) and (c) of the Clinger-Cohen Act have been re-codified in 40 USC, subtitle III, section 11315.

the DoD CIO will provide for elimination of duplicate IT and national security systems within and between Military Departments and Defense agencies. The Military Department CIOs will review budget requests for all IT and national security systems and ensure that IT and national security systems are interoperable with other relevant IT and national security systems within the government and DoD.

OMB Circular A-130. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000, establishes IRM policy. OMB Circular A-130 requires agencies to appoint a CIO who must report directly to the agency Head to carry out responsibilities of agencies listed in the Paperwork Reduction Act, Clinger-Cohen Act, and Executive Order 13011. The Military Departments and the Office of the Secretary of Defense may each appoint one official. The CIO must monitor and evaluate performance of information resource investments and advise the agency Head on whether to continue, modify, or terminate a program or project.

Appendix E. Principal Staff Assistants

DoD has designated elements of the Office of the Secretary of Defense as Principal Staff Assistants and advisors to the Secretary and Deputy Secretary of Defense for key functional areas within DoD. Pertinent Principal Staff Assistants and their functional area responsibilities include:

- Under Secretary of Defense for Acquisition, Technology, and Logistics is the Principal Staff Assistant and advisor to the Secretary and Deputy Secretary of Defense for all matters relating to the DoD Acquisition Systems, research and development; advanced technology; developmental test and evaluation; production; logistics; installation management; military construction; procurement; environmental security; and nuclear, chemical, and biological matters;

- Under Secretary of Defense (Comptroller)/Chief Financial Officer is the Principal Staff Assistant and advisor to the Secretary and Deputy Secretary of Defense for budgetary, fiscal, and program analysis and evaluation matters (including financial management, accounting policy and systems, management control systems, budget formulation and execution, and contract audit administration and organization), and general management improvement programs;

- Under Secretary of Defense for Personnel and Readiness is the Principal Staff Assistant and advisor to the Secretary and Deputy Secretary of Defense for Total Force management as it relates to readiness; National Guard and Reserve component affairs; health affairs; training; and personnel requirements and management, including equal opportunity, morale, welfare, recreation, and quality of life matters; and

- ASD(NII)/DoD CIO is the Principal Staff Assistant and advisor to the Secretary and Deputy Secretary of Defense for networks and network-centric policies and concepts; command and control; communications; non-intelligence space matters; enterprise-wide integration of DoD information matters; IT, including national security systems; IRM; spectrum management; network operations; information systems; information assurance; positioning, navigation, and timing policy, including airspace and military-air-traffic control activities; sensitive information integration; contingency support and migration planning; and related matters.

Appendix F. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
    Director, Business Transformation Program Management Office
Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Under Secretary of Defense for Personnel and Readiness
Under Secretary of Defense for Intelligence
Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer
Director, Program Analysis and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)

Other Defense Organization

Director, Defense Information Systems Agency

Non-Defense Federal Organization

Office of Management and Budget

.

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Acquisition and Technology Management Directorate prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Mary Ugone
Kathryn Truex
Sarah Davis
Tracy Smelley
Barry Gay
James Buscaglio